AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Previously presented) A method of securing access to resources in a computing device, comprising the steps of:

storing an encrypted access code in a memory location within the computing device;

receiving a password to access the resources;

encrypting the password to produce a encrypted password;

comparing the encrypted password to the encrypted access code;

allowing access to the resources if the encrypted access code matches the encrypted password.

2. (Original) The method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

3. (Original) The method of claim 2 wherein the step of encrypting a password comprises the step of hashing a password.

4. (Original) The method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified.

5. (Original) The method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password.

6. (Original) The method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password.

7. (Currently amended) A computing device comprising:

a processing system;

a memory coupled to the processing system for storing an encrypted access code;

input circuitry coupled to the processing system for receiving a password to access resources;

wherein the processing circuitry:

encrypts the password to produce a encrypted password;

compares the encrypted password to the encrypted access code;

allows access to the resources if the encrypted access code matches the encrypted password.

8. (Original) The computing device of claim 7 wherein the encrypted access code comprises a hashed access code.

9. (Original) The computing device of claim 8 wherein the encrypted password comprises a hashed password.

10. (Original) The computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified.

11. (Original) The computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

12. (Original) The computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password.

13. (Previously presented) The method of claim 1 wherein the memory location is within a processing system in the computing device.

14. (Previously presented) The method of claim 13, wherein the processing system is a baseband processing system.

15. (Previously presented) The method of claim 13 wherein the memory location is in a memory subsystem within the processing system.

16. (Previously presented) The method of claim 15 wherein the memory subsystem comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

17. (Previously presented) The method of claim 16 further including at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array.

18. (Previously presented) The method of claim 16 wherein some portions of the memory array are externally accessible but not modifiable.

19. (Previously presented) The method of claim 16 wherein some portions of the memory array are not externally accessible and are not modifiable.

20. (Previously presented) The method of claim 16 wherein an encryption key is stored in the memory array.

21. (Previously presented) The method of claim 20 wherein the encryption key is generated by a random number generator internal to the processing system.

22. (Previously presented) The method of claim 21 wherein the encryption key is generated at the time of production of the processing system.

23. (Previously presented) The method of claim 15, further including at least one processor coupled to the memory subsystem.

24. (Previously presented) The method of claim 23, further including a non-volatile memory system coupled to the processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device.

25. (Previously presented) The method of claim 24, further including a radio frequency (RF) system coupled to the processing system.

26. (Previously presented) The method of claim 16, further comprising at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number.

27. (Previously presented) The method of claim 17 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data

associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

28. (Previously presented) The method of claim 24, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate.

29. (Previously presented) The method of claim 1 wherein the encrypted password is of a different length than the received password.

30. (Previously presented) The computing device of claim 7 wherein the memory is a memory subsystem within the computing device.

31. (Previously presented) The computing device of claim 30 wherein the processing system, the memory and the input/output comprise a baseband processing system.

32. (Previously presented) The computing device of claim 31 wherein the memory location is in a memory subsystem within the baseband processing system.

33. (Previously presented) The computing device of claim 32 wherein the memory subsystem comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

34. (Previously presented) The computing device of claim 33 further including at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array.

35. (Previously presented) The computing device of claim 33 wherein some portions of the memory array are externally accessible but not modifiable.

36. (Previously presented) The computing device of claim 33 wherein some portions of the memory array are not externally accessible and are not modifiable.

37. (Previously presented) The computing device of claim 33 wherein an encryption key is stored in the memory array.

38. (Previously presented) The computing device of claim 37 wherein the encryption key is generated by a random number generator internal to the processing system.

39. (Previously presented) The computing device of claim 38 wherein the encryption key is generated at the time of production of the processing system.

40. (Previously presented) The computing device of claim 33, further including at least one processor coupled to the memory subsystem.

41. (Previously presented) The computing device of claim 31, further including a non-volatile memory system coupled to the baseband processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device.

42. (Previously presented) The computing device of claim 41, further including a radio frequency (RF) system coupled to the baseband processing system.

43. (Previously presented) The computing device of claim 34, further comprising at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number.

44. (Previously presented) The computing device of claim 35 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

45. (Previously presented) The computing device of claim 41, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate.

46. (Previously presented) The computing device of claim 7 wherein the encrypted password is of a different length than the received password.